What is OPSEC?

Operations Security (OPSEC) is an analytic process used to deny an adversary information - generally unclassified - concerning our intentions and capabilities by identifying, controlling, and protecting indicators associated with our planning processes or operations. OPSEC does not replace other security disciplines - it supplements them.

OPSEC – A New Mindset

- Our attention to security must change now. The events of September 11th, 2001 proved there is a demonstrated and known threat. How many times have we heard that terrorism is a threat? But, most of us thought it could only happen elsewhere – not in America.
- Unfortunately, we have suffered several terrorist attacks in recent years - the Oklahoma City and U.S.S. Cole attacks, and the tragic events that unfolded on September 11, 2001. In these cases, the adversary was successful because they knew our vulnerabilities. Americans at large provided much of what was used against us. The only thing our enemies brought to the table was their personal agenda and their resolve.
- As Federal employees, we are the representatives of the people. We develop, we plan, we execute - the American people trust us to do our jobs and keep them safe. The mishandling of information can put everything at risk and cost the lives of many Americans.

Why is it important that we learn about OPSEC?

- The information that is often used against us is not classified information; it is information that is openly available to anyone who knows where to look and what to ask.

- Operations Security is a tool that our adversaries believe in ... and one that we in the United States Government need to understand and integrate into our daily routine. Our work is information, and not all of it is classified. What we don't always realize is how much we are giving away by our predictable behavior, casual conversations, routine acquisitions and other Internet information. We must be careful of what we are revealing - failure to do so could provide our adversaries with the information they need to execute additional terrorist acts.

What can I do to help thwart any further attempts to harm the U.S.A?

We can all incorporate OPSEC into our everyday work routine. Practicing operations security will help you accomplish your goals. When you do something, ask yourself, "What could an adversary glean from the knowledge of this activity? Is it revealing information about what we do and how we do it?" It is helpful to view yourself and what you're doing as an adversary would. For example, what can be gained by observing your actions or reading what you place on a website?

What are OPSEC indicators?

What do people observe about your schedule? What do you do when you go to work? What are you revealing by your predictable routines and the way you do business - these are indicators. OPSEC helps people identify the indicators that are giving away information about missions, activities, and operations.

Who is the adversary?

- Let's not focus strictly on terrorists right now. Remember that there are other adversaries - for example, foreign intelligence services that continue to collect information on us that could be used to hurt us in the future.
- We sometimes only focus on what just happened - but it is a certainty that our adversaries will continually look for and find any weak links.

What are the capabilities of our adversary?

We can *never* underestimate the capabilities or strength of conviction of terrorists or any other adversary. Nothing is more dangerous than people who are willing to die for a cause.

What is the risk?

The terrorist threat existed prior to September 11th, 2001. We just **did not believe** that such a horrific thing could ever happen. Everything we do involves risk - the application of the OPSEC process develops effective countermeasures to help us accomplish our future missions - by analyzing and minimizing the risk that we may inadvertently reveal critical information to our adversaries.

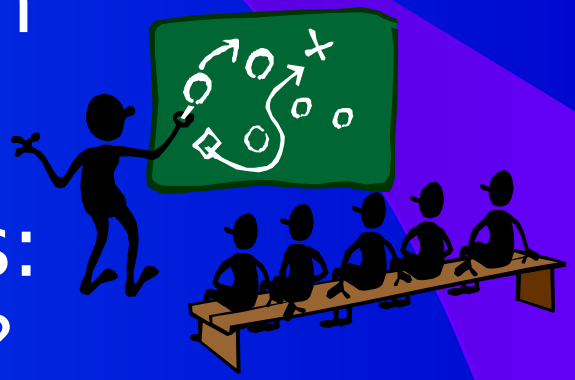
From the Interagency OPSEC Support Staff (IOSS)

Our enemy took *us* by surprise and we will never be the same country again. In order to effectively bring the enemy to justice, *we* need to maintain the element of surprise. Every element of our operation is more sensitive than ever before. We must rededicate ourselves to our mission and our country to help ensure that what transpired on September 11th will not be repeated. Security must be incorporated into every aspect of our jobs. If we are not vigilant in protecting critical information, it *will* happen again. The future of America depends on changing the way we look at security. OPSEC can make the difference. It is absolutely essential that it be understood and incorporated into everything we do.

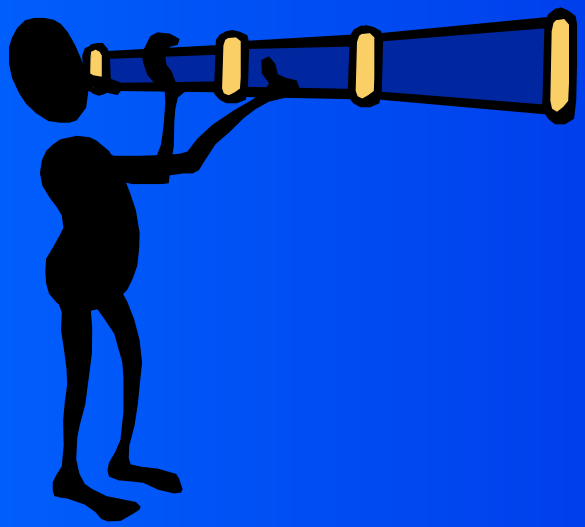
Introduction to Operations Security

Introduction

- Operations Security (OPSEC)
- Not a security program
- Is a mindset
- Answers the questions:
  - Who are the bad guys?
  - What do they want from me (us)?
  - How do they get it?
  - How can you help stop them?



Who are the bad guys?



- Enemies
- Competitors
- Terrorists
- Criminals
- Insiders

Intent & Capability = "THREAT"

Threats

- Terrorist threat
  - Targets fit their priorities
  - Demonstrated intent to hurt the U.S.
  - Capable of collecting unprotected information
  - Capable of acting on information
  - Do you (your organization) fit the profile?

Threats

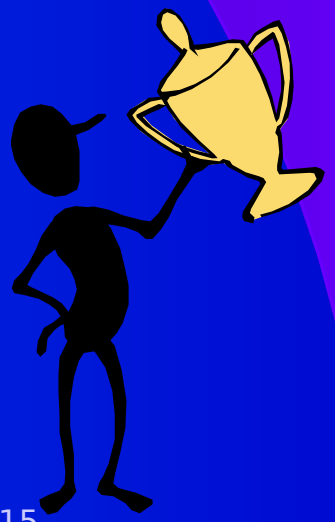
- Foreign Intelligence Threat
  - Military, economic, technology targets
  - Demonstrated intent to collect
  - Wide range in capability to collect and to act on information

What do they want from us?

"Critical Information"

- Information the adversary needs to *prevent* our success.

- Information we must protect to *ensure* success.



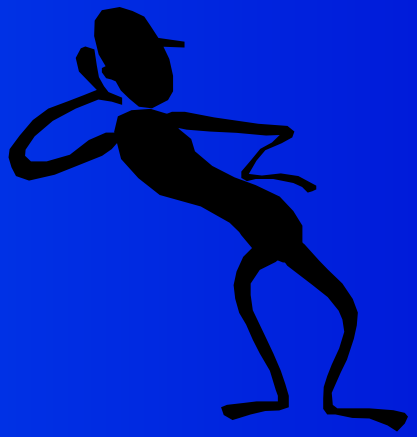
Critical Information

- Our limitations
- Specific operations plans
  - Who, what, when, where, how
- Our personnel & their families
- Our security process

How do they get it?

Bad guys' collection methods:

- Communications intercept
- Pictures
- Internet
- Elicitation
- Espionage



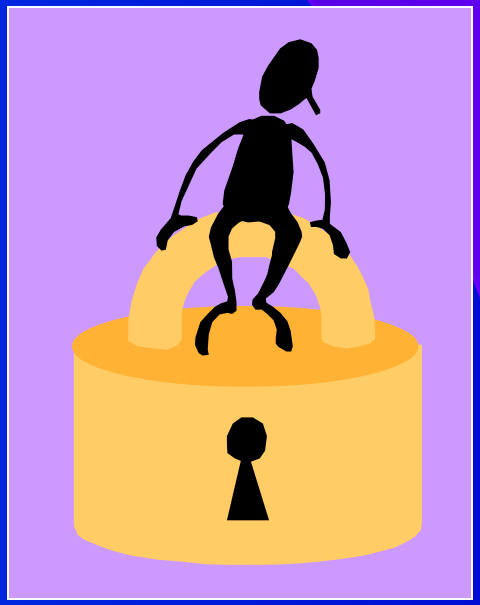
Illegal methods are OK with bad guys !!!

How do they get it?

- We give it to them! ("Vulnerabilities")
  - Web pages
  - Blogs
  - Email
  - Unprotected communications
  - Sharing too much with strangers

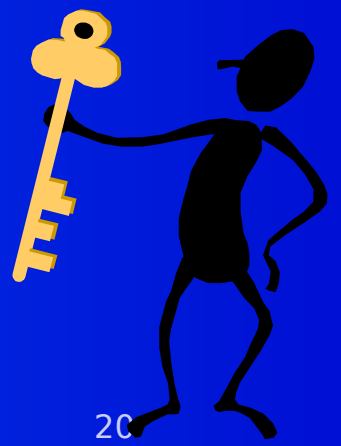
How can you help stop them?

- "Countermeasures"
  - Protected communications
  - Web page policies
  - Be alert
  - Be suspicious
  - Be aware

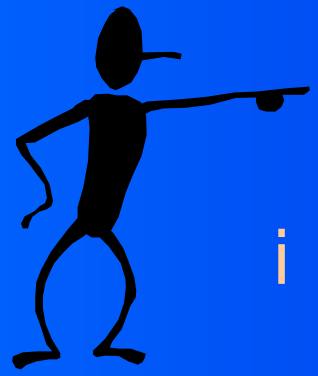


Countermeasures

- Consider the threat when you:
  - Use the phone
  - Answer stranger's questions
  - Discuss work in public places
- Practice good security
- Shred all paper



OPSEC Policy



- Our Critical Information
- Threats to our operation
- Our Countermeasures